SA Seksi 314

PENENTUAN RISIKO DAN PENGENDALIAN INTERN-PERTIMBANGAN DAN KARAKTERISTIK SISTEM INFORMASI KOMPUTER

Sumber: PSA No. 60

PENDAHULUAN

01. Dalam Seksi 335 [PSA No. 57] *Auditing dalam Lingkungan Sistem Informasi Komputer (SIK) didefinisikan sebagai berikut:*

    "Untuk tujuan Seksi ini, suatu lingkungan SIK ada bila suatu komputer dengan tipe atau ukuran apa pun digunakan dalam pengolahan informasi keuangan suatu entitas yang signifikan bagi audit, terlepas apakah komputer tersebut dioperasikan oleh entitas tersebut atau oleh pihak ketiga."

    Penggunaan semua pengendalian SIK yang disyaratkan mungkin tidak praktis bila ukuran bisnis adalah kecil atau bila komputer mikro digunakan tanpa melihat ukuran bisnis. Juga bila data diolah oleh pihak ketiga, pertimbangan karakteristik lingkungan SIK dapat tergantung atas tingkat akses ke pengolahan yang dilakukan oleh pihak ketiga tersebut.

STRUKTUR ORGANISASI

02. Dalam lingkungan SIK, entitas akan membentuk struktur organisasi dan prosedur untuk mengelola aktivitas SIK. Karakteristik suatu organisasi SIK adalah sebagai berikut:

    a. *Pemutusan fungsi dan pengetahuan*-meskipun semua sistem yang menggunakan metode SIK akan mencakup operasi manual tertentu, umumnya jumlah orang yang terlibat dalam pengolahan informasi keuangan sangat berkurang. Disamping itu, karyawan pengolahan data tertentu mungkin merupakan satu-satunya orang yang memiliki pengetahuan rinci tentang saling hubungan antara sumber data, bagaimana data tersebut diolah, dan keluarannya didistribusikan serta digunakan. Juga terdapat kemungkinan mereka menyadari adanya kelemahan pengendalian intern dan, oleh karena itu, mereka dalam posisi untuk mengubah program atau data selama disimpan atau diolah. Disamping itu, banyak pengendalian konvensional yang mungkin tidak ada, misalnya pengendalian yang didasarkan atas pemisahan fungsi yang tidak sejalan, atau dapat kurang efektif, dalam keadaan tidak adanya pengendalian terhadap akses atau pengendalian yang lain.
    b. *Pemutusan program dan data*-data transaksi dan data *file* induk seringkali dipusatkan, biasanya dalam bentuk yang dapat dibaca dengan mesin, yang dapat berada dalam instalasi komputer yang ditempatkan secara terpusat atau di beberapa instalasi yang disebar di seluruh lokasi dalam entitas. Program komputer yang memungkinkan pemakai berkemampuan untuk mengubah atau memperoleh akses ke data tersebut, kemungkinan disimpan dalam tempat yang sama dengan lokasi data. Oleh karena itu, dalam keadaan tidak adanya pengendalian yang semestinya, terdapat potensi yang semakin meningkat terjadinya akses tanpa izin ke, atau pengubahan terhadap, program dan data.

SIFAT PENGOLAHAN

03. Penggunaan komputer dapat menghasilkan desain sistem yang menyediakan lebih sedikit bukti yang dapat dilihat bila dibandingkan dengan yang dihasilkan dengan menggunakan prosedur manual. Disamping itu, sistem tersebut dapat diakses oleh orang dalam jumlah yang lebih banyak. Karakteristik sistem sebagai akibat dari sifat SIK adalah:

    a. *Tidak adanya dokumen masukan* – data dapat dimasukkan secara langsung ke dalam sistem komputer tanpa dokumen pendukung. Dalam beberapa sistem transaksi *on-line,* bukti tertulis untuk setiap otoritas *entry* data individual (misalnya pengesahan *entry* order dalam *on-line sistem*) dapat digantikan dengan prosedur lain, seperti pengendalian otoritas dalam program komputer (contohnya adalah pengesahan batas kredit).
    b. *Tidak adanya jejak transaksi (transaction trail)* – data tertentu hanya dapat disimpan dalam *file* komputer. Dalam sistem manual, umumnya terdapat kemungkinan untuk mengikuti suatu transaksi melalui sistem dengan memeriksa dokumen sumber, buku pembantu, catatan *file*, dan laporan. Namun, dalam lingkungan SIK, jejak transaksi dapat sebagian berbentuk *file*, dan laporan. Namun, dalam lingkungan SIK, jejak transaksi dapat sebagian berbentuk *file* yang hanya dapat dibaca dengan mesin, dan disamping itu, *file* tersebut hanya ada untuk jangka waktu yang terbatas.
    c. *Tidak adanya keluaran yang dapat dilihat dengan mata* – data dan program komputer dapat diakses dan diubah di komputer atau melalui penggunanaan ekuipmen komputer yang berada di lokasi yang jauh. Oleh karena itu, tidak adanya pengendalian semestinya, akan meningkatkan secara potensial akses tanpa otoritas ke, dan pengubahan terhadap, data dan program oleh orang di dalam atau di luar entitas.

ASPEK DESAIN DAN PROSEDUR

04. Pengembangan sistem SIK biasanya akan menghasilkan karakteristik dalam desain dan prosedur yang berbeda dengan yang dijumpai dalam sistem manual. Perbedaan tersebut mencakup:

    a. *Kinerja yang konsisten* – sistem SIK melaksanakan fungsi secara tepat sesuai dengan yang diprogram dan secara potensial lebih andal dibandingkan dengan sistem manual, dengan syarat bahwa semua tipe transaksi dan kondisi yang dapat terjadi diantisipasi dan dimasukkan ke dalam sistem tersebut. Di lain pihak, suatu program komputer yang diprogram dan diuji secara keliru dapat mengolah transaksi atau data lain secara konsisten salah.
    b. *Prosedur pengendalian terprogram* – sifat pengolahan komputer memungkinkan desain prosedur pengendalian dalam program komputer. Prosedur ini dapat didesain untuk menyediakan pengendalian dapat dilihat secara terbatas (seperti perlindungan data dari akses yang tanpa izin dapat disediakan melalui penggunaan *passwords*). Prosedur lain dapat didesain untuk digunakan dengan campur tangan manual, seperti *review* atas laporan tercetak untuk pelaporan kekeliruan dan penyimpangan, serta pengecekan kewajaran dan batas (*reasonableness and limit check*).
    c. *Pemutakhiran transaksi tunggal ke database file komputer atau berbagai file kompuer* – masukan tunggal ke dalam sistem akuntansi dapat secara otomatis memutakhirkan semua catatan yang berhubungan dengan transaksi tersebut (seperti, dokumen pengiriman barang dapat memutakhirkan *file* penjualan dan *file* piutang usaha, serta *file* sediaan). Jadi, kekeliruan *entry* ke dalam sistem tersebut akan mengakibatkan kekeliruan di berbagai akun keuangan.
    d. *Transaksi yang ditimbulkan oleh sistem* – transaksi tertentu dapat ditimbulkan oleh sistem SIK sendiri tanpa memerlukan dokumen masukan. Otoritas atas transaksi tersebut tidak dapat dibuktikan dengan dokumentasi masukan yang dapat dilihat atau tidak didokumentasikan dengan cara yang sama dengan transaksi yang ditimbulkan di luar sistem SIK (seperti bunga dapat dihitung dan dibebankan secara otomatis ke saldo akun pelanggan atas dasar syarat yang telah diotorisasi sebelumnya yang dimasukkan dalam program komputer).

e. *Rentannya media yang digunakan untuk menyimpan data dan program* – volume data dalam jumlah besar dan program yang digunakan untuk mengolah data tersebut dapat disimpan dalam media penyimpanan yang mudah dipindahkan atau yang tetap, seperti pita atau *disk* magnetis. Media ini rentan terhadap pencurian, penghancuran yang disengaja atau kecelakaan.

PENGENDALIAN INTERN DALAM LINGKUNGAN SIK

05. Pengendalian intern atas pengolahan komputer, yang dapat membantu pencapaian tujuan pengendalian intern secara keseluruhan, mencakup baik prosedur manual maupun prosedur yang didesain dalam program komputer. Prosedur pengendalian manual dan komputer terdiri atas pengendalian menyeluruh yang berdampak terhadap lingkungan SIK (pengendalian umum SIK) dan pengendalian khusus atas aplikasi akuntansi (pengendalian aplikasi SIK).

PENGENDALIAN UMUM SIK

06. Tujuan pengendalian umum (*general control*) SIK adalah untuk membuat rerangka pengendalian menyeluruh atas aktivitas SIK dan untuk memberikan tingkat keyakinan memadai bahwa tujuan pengendalian intern secara keseluruhan dapat tercapai. Pengendalian umum meliputi:

a. *Pengendalian organisasi dan manajemen* – didesain untuk menciptakan rerangka organisasi aktivitas SIK, yang mencakup:
   (1) Kebijakan dan prosedur yang berkaitan dengan fungsi pengendalian.
   (2) Pemisahan semestinya fungsi yang tidak sejalan (seperti penyiapan transaksi masukan, pemrograman, dan operasi komputer).

b. *Pengendalian terhadap pengembangan dan pemeliharaan sistem aplikasi* – didesain untuk memberikan keyakinan memadai bahwa sistem dikembangkan dan dipelihara dalam suatu cara yang efisien dan melalui proses otorisasi semestinya. Pengendalian ini juga didesain untuk menciptakan pengendalian atas:
   (1) Pengujian, perubahan, implementasi, dan dokumentasi sistem baru atau sistem yang direvisi.
   (2) Perubahan terhadap sistem aplikasi.
   (3) Akses terhadap dokumentasi sistem.
   (4) Pemerolehan sistem aplikasi dan *listing program* dari pihak ketiga.

c. *Pengendalian terhadap operasi sistem* – didesain untuk mengendalikan operasi sistem dan untuk memberikan keyakinan memadai bahwa:
   (1) Sistem digunakan hanya untuk tujuan yang telah diotorisasi.
   (2) Akses ke operasi komputer dibatasi hanya bagi karyawan yang telah mendapat otorisasi.
   (3) Hanya program yang telah diotorisasi yang digunakan.
   (4) Kekeliruan pengolahan dapat dideteksi dan dikoreksi.

d. *Pengendalian terhadap perangkat lunak sistem* – didesain untuk memberikan keyakinan memadai bahwa perangkat lunak sistem diperoleh atau dikembangkan dengan cara yang efisien dan melalui proses otorisasi semestinya, termasuk:
   (1) Otorisasi, pengesahan, pengujian, implementasi, dan dokumentasi perangkat lunak sistem baru dan modifikasi perangkat lunak sistem.
   (2) Pembatasan akses terhadap perangkat lunak dan dokumentasi sistem hanya bagi karyawan yang telah mendapatkan otorisasi.

e. *Pengendalian terhadap entry data dan program* – didesain untuk memberikan keyakinan bahwa:
   (1) Struktur otorisasi telah ditetapkan atas transaksi yang dimasukkan ke dalam sistem.
   (2) Akses ke data dan program dibatasi hanya bagi karyawan yang telah mendapatkan otorisasi.

07. Terdapat penjagaan keamanan SIK yang lain yang memberikan kontribusi terhadap kelangsungan pengolahan SIK. Hal ini meliputi:

    a. Pembuatan cadangan data program komputer di lokasi di luar perusahaan.
    b. Prosedur pemulihan untuk digunakan jika terjadi pencurian, kerugian, atau penghancuran data baik yang disengaja maupun yang tidak disengaja.
    c. Penyediaan pengolahan di lokasi di luar perusahaan dalam hal terjadi bencana.

PENGENDALIAN APLIKASI SIK

08. Tujuan pengendalian aplikasi (*application control*) SIK adalah untuk menetapkan prosedur pengendalian khusus atas aplikasi akuntansi untuk memberikan keyakinan memadai bahwa semua transaksi telah diotorisasi dan dicatat, serta diolah seluruhnya, dengan cermat, dan tepat waktu. Pengendalian aplikasi mencakup:

    a. *Pengendalian atas masukan* – didesain untuk memberikan keyakinan memadai bahwa:
        (1) Transaksi diotorisasi sebagaimana semestinya sebelum diolah dengan komputer.
        (2) Transaksi diubah dengan cermat ke dalam bentuk yang dapat dibaca mesin dan dicatat dalam *file* data komputer.
        (3) Transaksi tidak hilang, ditambah, digandakan, atau diubah tidak semestinya.
        (4) Transaksi yang keliru ditolak, dikoreksi, dan jika perlu, dimasukkan kembali secara tepat waktu.

    b. *Pengendalian atas pengolahan dan file data komputer* – didesain untuk memberikan keyakinan memadai bahwa:
        (1) Transaksi, termasuk transaksi yang dipicu melalui sistem, diolah semestinya oleh komputer.
        (2) Transaksi tidak hilang, ditambah, digandakan, atau diubah tidak semestinya.
        (3) Kekeliruan pengolahan diidentifikasi dan dikoreksi secara tepat waktu.

    c. *Pengendalian atas keluaran* – didesain untuk memberikan keyakinan memadai bahwa:
        (1) Hasil pengolahan adalah cermat
        (2) Akses terhadap keluaran dibatasi hanya bagi karyawan yang telah mendapatkan otorisasi.
        (3) Keluaran disediakan secara tepat waktu bagi karyawan yang mendapatkan otorisasi semestinya.

    d. *Pengendalian masukan, pengolahan, dan keluaran dalam sistem on-line*
        (1) Pengendalian masukan pada sistem *on-line* – didesain untuk memberikan keyakinan bahwa:
            - Transaksi di-*entry* ke terminal yang semestinya.
            - Data di-*entry* dengan cermat.
            - Data di-*entry* ke periode akuntansi yang semestinya.
            - Data yang di-*entry* telah diklasifikasikan dengan benar dan pada nilai transaksi yang sah (*valid*).
            - Data yang tidak sah (*invalid*) tidak di-*entry* pada saat transmisi.
            - Transaksi tidak di-*entry* lebih dari sekali.
            - Data yang di-*entry* tidak hilang selama masa transmisi berlangsung.
            - Transaksi yang tidak berotorisasi tidak di-*entry* – didesain untuk memberikan keyakinan.
        (2) Pengendalian pengolahan pada sistem *on-line* – didesain untuk memberikan keyakinan bahwa:
            (i) Hasil penghitungan telah diprogram dengan benar.
            (ii) Logika yang digunakan dalam proses pengolahan adalah benar.
            (iii) *File* yang digunakan dalam proses pengolahan adalah benar.
            (iv) *Record* yang digunakan dalam proses pengolahan adalah benar
            (v) Operator telah memasukkan data ke komputer *console* yang semestinya.
            (vi) Tabel yang digunakan selama proses pengolahan adalah benar.

(vii) Selama proses pengolahan telah digunakan standar operasi (*default*) yang semestinya.
(viii) Data yang tidak sah tidak digunakan dalam proses pengolahan.
(ix) Proses pengolahan tidak menggunakan program dengan versi yang salah.
(x) Hasil penghitungan yang dilakukan secara otomatis oleh program adalah sesuai dengan kebijakan manajemen entitas.
(xi) Data masukan yang diolah adalah data yang berotorisasi.

(3) Pengendalian keluaran pada sistem *on-line* – didesain untuk memberikan keyakinan bahwa:
(i) Keluaran yang diterima oleh entitas adalah tepat dan lengkap.
(ii) Keluaran yang diterima oleh entitas adalah terklasifikasi.
(iii) Keluaran didistribusikan ke personel yang berotorisasi.

REVIEW ATAS PENGENDALIAN UMUM SIK

09. Pengedalian umum SIK yang diuji oleh auditor telah dijelaskan dalam paragraf 06. Auditor harus mempertimbangkan bagaimana pengendalian umum SIK yang berdampak terhadap aplikasi SIK signifikan bagi auditnya. Pengendalian umum SIK yang berhubungan dengan beberapa atau seluruh aplikasi merupakan pengendalian yang saling terkait yang operasinya seringkali merupakan hal yang menentukan efektivitas pengendalian aplikasi SIK. Oleh karena itu, adalah lebih efisien untuk me-*review* desain pengendalian umum lebih dahulu sebelum auditor melakukan *review* terhadap pengendalian aplikasi.

REVIEW ATAS PENGENDALIAN APLIKASI

10. Pengendalian atas masukan, pengolahan, *file* data, dan keluaran dapat dilaksanakan oleh karyawan SIK, oleh pemakai sistem, oleh grup pengendali terpisah, atau dapat diprogram ke dalam perangkat lunak aplikasi. Pengendalian aplikasi SIK, yang diuji oleh auditor mencakup:

a. *Pengendalian manual yang dilaksanakan oleh pemakai* – Jika pengendalian manual yang dilakukan oleh pemakai sistem aplikasi mampu memberikan keyakinan memadai bahwa keluaran sistem lengkap, cermat, dan terotorisasi, auditor dapat memutuskan untuk membatasi pengujian pengendaliannya terhadap pengendalian manual tersebut (seperti pengendalian manual yang dilakukan oleh pemakai atas sistem penggajian terkomputerisasi bagi karyawan dapat mencakup total pengendalian masukan, pengecekan terhadap perhitungan keluaran gaji bersih, persetujuan pembayaran dan transfer dana, perbandingan ke jumlah daftar gaji, dan rekonsiliasi bank dengan segera). Dalam hal ini, auditor dapat melakukan untuk pengujian hanya terhadap pengendalian manual yang dilaksanakan oleh pemakai.
b. *Pengendalian atas keluaran sistem* – jika, di samping pengendalian masukan yang dilaksanakan oleh pemakai, pengendalian yang harus diuji menggunakan informasi yang dihasilkan oleh komputer atau termasuk dalam program komputer, kemungkinan auditor dapat menguji pengendalian tersebut dengan memeriksa keluaran sistem dengan menggunakan teknik manual atau teknik audit berbantuan komputer. Keluaran tersebut dapat berbentuk media magnetis, *microfilm* atau cetakan (seperti, auditor dapat menguji pengendalian yang dilaksanakan oleh entitas atas rekonsiliasi total laporan ke dalam akun kontrol yang bersangkutan dalam buku besar dan dapat melakukan pengujian manual terhadap rekonsiliasi tersebut). Sebagai alternatif, bila rekonsiliasi dilaksanakan dengan komputer, auditor dapat melakukan pengujian atas rekonsiliasi tersebut dengan melaksanakan kembali pengendalian tersebut dengan menggunakan teknik audit berbantuan komputer. Lihat SA Seksi 327 [PSA No. 59] *Teknik Audit Berbantuan Komputer.*

c. *Prosedur pengendalian terprogram* – dalam sistem komputer tertentu, auditor dapat menjumpai keadaan yang di dalamnya ia tidak mungkin atau, dalam beberapa hal, tidak praktis untuk menguji pengendalian dengan hanya memeriksa pengendalian oleh pemakai atau keluaran sistem (seperti dalam aplikasi yang tidak menghasilkan keluaran atau mengesampingkan kebijakan normal, auditor mungkin ingin menguji prosedur pengendalian yang terdapat dalam program komputer). Auditor dapat mempertimbangkan pelaksanaan pengujian pengendalian dengan menggunakan teknik audit berbantuan komputer, seperti data uji, data transaksi yang diproses kembali atau, dalam situasi yang tidak biasa, memeriksa pengkodean program aplikasi.

EVALUASI

11. Pengendalian umum SIK dapat memiliki dampak luas atas pengolahan transaksi dalam sistem aplikasi. Jika pengendalian ini tidak efektif, maka akan terdapat risiko bahwa salah saji mungkin terjadi dan berlangsung tanpa dapat dideteksi dalam sistem aplikasi. Jadi, kelemahan dalam pengendalian umum SIK menghalangi pengujian pengendalian aplikasi SIK tertentu; namun, prosedur manual yang dilaksanakan oleh pemakai dapat memberikan pengendalian efektif pada tingkat aplikasi.

TANGGAL BERLAKU EFEKTIF

12. Seksi ini berlaku efektif tanggal 1 Agustus 2001. Penerapan lebih awal dari tanggal efektif berlakunya aturan dalam Seksi ini diizinkan. Masa transisi ditetapkan mulai dari 1 Agustus 2001 sampai dengan 31 Desember 2001. Dalam masa transisi tersebut berlaku standar yang terdapat dalam Standar Profesional Akuntan Publik per 1 Agustus 1994 dan Standar Profesional Akuntan Publik per 1 Januari 2001. Setelah tanggal 31 Desember 2001, hanya ketentuan dalam Seksi ini yang berlaku.